DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Office of IT Field Security Operations and
Office of Risk Management & Incident Response

Monthly Report to Congress of Data Incidents

October 31 - December 4, 2011

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068163	Mishandled/ Misused Physical or Verbal Information	VISN 04 Butler, PA	10/31/2011	11/2/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	10/31/2011	INC000000179500	N/A	N/A	N/A	1	

Incident Summary

Veteran A received two radiology appointment letters in the mail. One letter was correctly addressed to him and the other letter was for Veteran B. The letter contained Veteran B's full name, last four digits of the social security number, date of birth, and address. Veteran A shredded the information and also called the supervisor of clinical services to inform him of the incident.

Incident Update

10/31/11:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 91 Mis-Mailed incidents this reporting period. Because of repetition, the other 90 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The supervisor of the area reminded staff to make sure the correct information is put in the correct envelopes.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068167	Missing/Stolen Equipment	VISN 12 Chicago, IL	10/31/2011	11/28/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	10/31/2011	INC000000179513	N/A	N/A	N/A		

Incident Summary

One monitor and two CPUs were reported stolen. No patient information or logs were stored on the hard drive. All patient information was stored electronically via VistA and CPRS.

Incident Update

11/08/11:
A VA Police report has been filed. The CPUs were not encrypted. The CPUs were used by two employees in the Flu Clinic and they have stated they did not store anything on the hard drives. The CPUs were last connected to the VA network on 10/28/11. A Report of Survey was completed. There is a very low risk of a data breach.

Resolution

No patient information or logs were stored on the hard drive. All patient information was stored electronically via VistA and CPRS.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068223	Mishandled/ Misused Physical or Verbal Information	VISN 09 Huntington, WV	11/1/2011	11/17/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/1/2011	INC000000179882	N/A	N/A	N/A		1

Incident Summary

Patient A was given Patient B's medication and reported the incident to the Pharmacy. Patient B's name, address and type of medication was compromised.

Incident Update

11/01/11:
Patient B will be sent a notification letter due to full name and protected health information (PHI) being exposed.

NOTE: There were a total of 102 Mis-Handling incidents this reporting period. Because of repetition, the other 101 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

Staff were reminded to be more cautious when packaging/dispensing medications.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068311	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	11/3/2011	12/8/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/3/2011	INC000000180342	N/A	N/A	N/A		1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. The packing error has been reported to Medline for investigation and corrective action.

Incident Update

11/04/11:
Patient B will be sent a letter of notification.

NOTE: There were a total of 12 Mis-Mailed CMOP incidents out of 7,671,159 total packages (11,194,036 total prescriptions) mailed out for this reporting period. Because of repetition, the other 11 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Resolution

The packing error has been reported to Medline for investigation and corrective action.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068326	Missing/Stolen Material (Non-Equipment)	VISN 23 Iowa City, IA	11/3/2011	11/17/2011		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/4/2011	INC000000180417	N/A	N/A	N/A	57	

Incident Summary

A VA employee reported papers containing 57 Veterans' names, dates of births, full SSNs along with personal tax information and a social security card was missing from a secure clinical call center. The VA Police were contacted and an investigation is in progress.

Incident Update

11/04/11:
Fifty-seven Veterans will be sent letters offering credit protection services.

Resolution

A high priority work order was placed to have the call center rekeyed. Only employees who work in the area and supervisor will have a key to this room. All protected health information (PHI) will be locked up overnight.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068373	Privacy	VISN 11 Indianapolis, IN	11/5/2011			Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	N/A	N/A	N/A	N/A	N/A	142	14

Incident Summary

A VA Social Worker's briefcase was stolen from a government vehicle. The Social Worker now believes it contained sensitive information (full name and full social security number) belonging to homeless Veterans. The number affected and names are being determined.

Incident Update

11/09/11:
The Social Worker is working to determine the names of Veterans affected, however it will be difficult to notify all of the Veterans since they are homeless.

11/09/11:
The list contained 142 living and 14 deceased Veterans' information, therefore 142 Veterans will receive a letter offering credit protection services and 14 Veteran's Next of Kin will receive a notification letter. Conspicuous notice will need to be posted due to the fact that these are homeless Veterans.

11/21/11:
The affected Veterans have been contacted by telephone. Letters and conspicuous notice will follow.

12/13/11:
All of the letters have been sent. This week posters will be placed in local homeless shelters and in the VA clinics that the homeless Veterans frequent. The posters are being made in house and will be posted for 90 days. The Privacy Officer has a written statement from the Social Worker and will turn the file over to Human Resources for their action.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068434	Missing/Stolen Equipment	VISN 17 San Antonio, TX	11/8/2011	11/14/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/8/2011	INC000000181062	N/A	N/A	N/A		

Incident Summary

On 09/29/11, a VA Warehouse Supervisor informed the VA Police Service that a laptop computer that was awaiting processing was missing and possibly stolen. This laptop was still in the box and didn't have any VA sensitive information on it.

Incident Update

11/08/11:
No data breach occurred. The laptop was brand new and had never been issued to a user.

Resolution

The laptops are locked down but are not, and cannot be, put away during the night. The Environmental Management Service (EMS) no longer has access to that area. The door locks and access badges access have been changed as well. The Privacy Office (PO) will ensure that the retraining of Human Resources (HR) personnel on Information Security and Privacy is documented.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068449	Missing/Stolen Equipment	VISN 20 Seattle, WA	11/8/2011	12/13/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/8/2011	2011-	N/A	N/A	N/A		

Incident Summary

During a regular IT inventory at a Community Based Outpatient Clinic (CBOC), a workstation was discovered missing. All workstations are cable-locked to the desk where they sit. Both the workstation and the cable lock were gone. It is unknown at what point this equipment went missing as the person using it left the VA and no one was using the office. All workstations are used to connect to servers and the C:\ drive is locked down. It is unlikely that any data was on the machine itself but the piece of equipment is gone.

Incident Update

11/09/11:
No data breach has occurred. The local hard drive C:\ is locked down by policy and any data would have been saved to the network servers.

NOTE: There were a total of 3 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 2 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

VA Police have physically searched Chehalis CBOC and Am-Lake, and GSA Auburn warehouse. The items were not located. The Chehalis CBOC staff is adamant that a VA Staff member swapped out the PC and Monitor on the same day around October 2010. VA Police have closed out this case and founded these items as lost, just as the service line has listed. A VA Police Report and a Report of Survey have been submitted to Facility Logistics staff.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068523	Missing/Stolen Equipment	VISN 17 San Antonio, TX	11/10/2011	12/8/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/10/2011	INC000000181610	N/A	N/A	N/A		

Incident Summary

The Information Security Officer (ISO) received a report of a missing smart wheel laptop computer that attaches to a wheelchair in the Poly-Trauma unit at the facility. The device appears to have been in the shipping box when taken. No one has seen it other than in the warehouse on or around 08/31/11. The VA Police Service is investigating and a Police Report is forthcoming. The Network ISO and the Associate Director are aware of this incident. No VA sensitive information is stored on this computer.

Incident Update

11/10/11:
No data breach occurred. The laptop was brand new and had never been issued to a user.

Resolution

The facility has not received any report of the recovery of the stolen smart wheel laptop, nor do they expect to. The Logistics Supervisor has committed to having his employees review and following the Standard Operating Procedure (SOP) of acquisitioning/inventorying new equipment.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068670	Mishandled/ Misused Physical or Verbal Information	VISN 16 Oklahoma City, OK	11/15/2011			Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/15/2011	INC000000182202	N/A	N/A	N/A		253

Incident Summary

At a Merit System Protection Board (MSPB) hearing, terminated Employee A came to testify on behalf of Employee B. Terminated Employee A brought a service consult list that was 3 pages long and contained 121 patients' names, last 4 digits of the SSN, request date and patient locations.

Incident Update

11/21/11:
The 121 patients will receive notification due to their protected health information (PHI) being maintained outside of VA control by the terminated employee. She was terminated on 11/21/10 for poor performance. The consult list is something she would have had access to in the course of her duties while she was employed at VA. The list was retrieved from terminated Employee A.

12/08/11:
The Privacy Officer ran that the report that the terminated Employee A brought to the MSPB hearing and found that the entire report contained information on 253 patients. VA is concerned that the ex-employee may still have the additional data in her possession. Therefore 253 patients will receive a letter of notification.

12/09/11:
The letters were printed and mailed today.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068806	Mishandled/ Misused Physical or Verbal Information	VISN 23 Omaha, NE	11/18/2011	12/13/2011		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/18/2011	INC000000183039	N/A	N/A	N/A	74	

Incident Summary

A resident from an affiliate hospital had a logbook stolen out of his vehicle at the affiliate hospital. This logbook contained information on all patients he has seen in the Omaha VAMC Operating Room (OR) for the past 20 months, so he could track his procedures and types of anesthetics he used. The resident stated that he would either just write in the patient's age, case, procedure type, and anesthetic used (with no identifiers) or in some instances he took a patient's label with their full name, SSN, and DOB and stuck it in the log. He does not know what patients were in his log.

Incident Update

11/21/11:
The Police Report was filed by the affiliate hospital not VA. The resident also sees patients at 3 other private sector hospitals and he is notifying appropriate staff at those facilities since the logbook included all patients seen by him at all 4 facilities.

11/30/11:
The Privacy Officer did a search of all the patients that the resident created an anesthesia report on and the number was 87. The 87 patients will receive a letter offering credit protection services.

12/08/11:
There were duplicate entries for some of the patients. The final number of patients offered credit protection is 74.

Resolution

The resident received additional training regarding protecting personally identifiable information (PII) and protected health information (PHI).

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068829	Mishandled/ Misused Physical or Verbal Information	VISN 20 Seattle, WA	11/18/2011			Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/18/2011	INC000000183134	N/A	N/A	N/A		

Incident Summary

A vulnerability was discovered on a shared listserv utilized by VA Puget Sound researchers, the Fred Hutchinson Cancer Research Center and possibly twenty-five other sites involved in Bone Marrow Transplant studies. An email/listserv was utilized by all twenty-five sites to share protected health information (PHI) and other research data. The Associate General Counsel for Fred Hutchinson Cancer Research Center contacted the Director, Human Research Protection Program that the "secured" email/listserv system utilized by the twenty-five research sites may have been "unsecured" since February 2009.

Incident Update

11/22/11:
The Privacy Officer (PO) is still awaiting word from the research group and Information Security Officer (ISO) in regards to the data elements that were unsecured and any other relevant information related to this ticket.

11/30/11:
Fred Hutchinson Cancer Research Center has confirmed that VA patient data was accessible to the public via the web. They have not yet confirmed a solid number. Right now we believe there are upwards of 40 patients. The relationship with VA is primarily research. Patients sign an Informed Consent and HIPAA Authorization for data use. There is a Memorandum of Understanding (MOU) which is currently being reviewed by Counsel for validity.

12/05/11:
A total of 44 patients can be identified whose name, full SSN and PHI including diagnosis, medication and lab results can be identified. These 44 patients will receive an offer for credit protection services. The emails were stopped, the data was removed from the web and they are looking into another method of communication.

Resolution

The Director's Office is convening an Administrative Investigation Board (AIB) to more fully investigate this incident. Training on privacy policies and procedures will be conducted in conjunction with the ISO and Research and Compliance Offices.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068857	Missing/Stolen Equipment	Corporate Data Center Operations (CDCO) Hines, IL	11/21/2011			Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/21/2011	INC000000183337	N/A	N/A	N/A		

Incident Summary

There is an investigation that is currently being conducted regarding 8 laptops that are missing and suspected stolen from building 215 at Hines on Friday 11/18/11. The VA Hines Police were called approximately 2:00 PM local time and left at about 4:30 PM local time after doing initial interviews. Hines Police are handling it as a criminal investigation. The theft was reported by one of the warehouse staff when he noticed that the inventory count of laptops didn't match to the physical count. The VBA technical management confirmed that the serial numbers of the missing laptops had not been deployed to the field and were still in the box, therefore no personally identifiable information (PII) or protected health information (PHI) was on the laptops.

Incident Update

11/21/11:
The laptops were all still in their boxes and had no VA data stored on them.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068873	Mishandled/ Misused Physical or Verbal Information	VISN 09 Huntington, WV	11/21/2011			Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/21/2011	INC000000183446	N/A	N/A	N/A		67

Incident Summary

When searching some lockers that had been retrieved from storage, our Chief Logistics and others found patient listings in one of the lockers. The locker had been stored at an offsite facility that is shared by the VA facility & active duty personnel.

Incident Update

11/28/11:
Employees from the medical center were checking lockers that had been stored at the local Base Realignment and Closure (BRAC) building. They discovered documents containing personally identifiable information (PII) on multiple patients. The room that these lockers were stored in is believed to have only been accessible by VA employees. However, it is believed that the lockers were removed from the VA inpatient areas and this would have been done by contractors. The facility is unable to identify who was responsible for leaving the documents in the lockers.

12/01/11:
All affected Veterans will be sent letters of notification as their names and medical information were left in these lockers for an undetermined amount of time. The first count is 109 Veterans but there are possible duplicates. When the list is put in a spreadsheet duplicates will be counted and the number will be reduced.

12/09/11:
Further investigation revealed that the lockers were moved from a health care employee area in or about May 2011 by VA employees and were relocated to a locked storage facility under control of VA Engineering. Although the potential breach of information cannot be confirmed, notification letters will be sent to the Veterans on the paper documents found.

The final count is 67 patients. Thirty two are deceased and their next of kin (NOK) will receive NOK notifications. The remaining thirty five will receive letters of notification.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000068927	Mishandled/ Misused Physical or Verbal Information	VISN 11 Battle Creek, MI	11/22/2011			Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	11/22/2011	INC000000183769	N/A	N/A	N/A		

Incident Summary

A Primary Care Provider removed "recyclable" material for use in a printer/fax machine in their private practice clinic. An unknown amount of records/papers were removed for an unknown number of Veterans. An anonymous complainant has produced one document containing a work schedule for the clinic on one side and a progress note on the other (indicating it had been run through the printer at the clinic). More investigation is needed to understand how many other Veterans may be impacted.

Incident Update

11/28/11:
The Privacy Officer (PO) is scheduled to inspect the practice and their records in the evening of 11/29/11. The PO will update with the findings the morning of 11/30/11.

12/02/11:
On 11/29/11 the Private Clinic in Coldwater, MI was inspected by the Battle Creek VAMC Privacy Officer and the Clinic Office Manager. During the inspection 12 VA Veteran medical records were discovered in administrative files and medical records that had other information printed on the blank side pertaining to the private clinic. The clinic manager and PO had agreed that there were too many records to be able to search all of them that evening and that a small team of people would be needed to complete the records search. The PO left the clinic with the records that had been discovered and informed the clinic manager that he would form a team and make arrangements with the clinic manager to gain access to the clinic ASAP. A team was formed and arrangements were made to have the Provider (a VA Primary Care Provider and the Private Clinic Owner) to be available and present for the inspection on 12/02/11. The Privacy Officer and a small team had agreed to meet the Provider at the private clinic at 1100 on 12/02/11. The team arrived at the Clinic in Coldwater and received a phone call from the Battle Creek VAMC ROI Office that a fax had been received from the Provider's attorney stating that the Provider would not consent to the search of the clinic and the VAMC team would not be permitted access to her private property. Due to the lack of cooperation on the Provider's part, the number of individuals affected by this breach cannot be realized at this time.

12/12/11:
OIG Special Agent in Charge was contacted and discussed the lack of cooperation and any recourse the VAMC may have to retrieve the medical records still in the private clinic. Regional Counsel was also contacted and has sent a letter to the Provider's attorney requesting the records be returned and the facility Information Security Officer (ISO) be allowed to inspect the clinic for VA records. The Provider has been placed on Administrative Leave pending a Professional Standards Board Investigation to be held on 12/16/11.

12/13/11:
The Privacy Officer spoke with Regional Counsel on 12/09/11. The Provider has agreed to return all the VA documents. The Privacy Officer is arranging for a meeting this Friday (12/16/11) to facilitate the retrieval of the documents. Once the documents are in VA custody, the Privacy Officer will be able to review and determine the exact count of affected individuals.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000069199	Missing/Stolen Material (Non-Equipment)	VISN 01 Boston, MA	12/1/2011	12/5/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	12/1/2011	INC000000185155	N/A	N/A	N/A		

Incident Summary

It has been reported by a staff psychologist that a VA purchased Toshiba Notebook computer has been missing from the third floor of 251 Causeway St. Room 330 since approximately 11/09/11. The psychologist stated that the laptop was last seen inside a secure lockable cabinet in Room 330 and she had assumed it was being used by another staff member when she could not locate it there. It was also stated that there was no patient information stored on the computer and it was only used to conduct PowerPoint presentations. The psychologist also stated that a general email was sent to all staff of the third floor and Psychiatry students to ask if someone had forgotten to return it. All staff stated they did not have it. The laptop was password protected and was never connected to the VA intranet or the internet.

Incident Update

12/01/11:
The laptop was purchased by Mental Health Service with Mental Health funds in June of 2007 and has never been on the VA network, joined to the VA domain, nor has it been encrypted. The laptop has only been used for PowerPoint presentations and does not contain any patient data.

Resolution

The issue has been reported to VA Police and investigated. The laptop did not contain any sensitive information.

Total number of Lost Blackberry Incidents	30
Total number of Internal Un-encrypted E-mail Incidents	113
Total number of Mis-Handling Incidents	102
Total number of Mis-Mailed Incidents	91
Total number of Mis-Mailed CMOP Incidents	12
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	18 (11 encrypted)